

Task 8 Marking Key: High Value Domestic Network Design Project

Marking Notes

Award marks for evidence that responds to the student's selected realestate.com.au property and floorplan. The UniFi Design Center evidence, topology explanation and written justification should align. Devices shown in the design should be explained, and major written recommendations should appear in the design evidence.

The project is marked out of 40 marks. Record raw marks only.

Criterion 1: Property Selection And Requirements Analysis

Expected response	Marks
Selects a suitable realestate.com.au house listing with a usable floorplan and records the source, including listing title or description, suburb, URL and date accessed.	1
Identifies property features or zones that affect the network design, such as study, bedrooms, living areas, garage, theatre, outdoor area or multiple storeys.	1
Identifies likely users and device categories for a high value domestic network, such as family users, guests, home office devices, entertainment devices, IoT devices or cameras.	1
Identifies high value network requirements such as coverage, performance, reliability, home office use, smart home use or guest access.	1
Identifies constraints or risks such as floorplan scale, wall materials, dead zones, cost, security or privacy.	1
States assumptions or limitations used when interpreting the floorplan.	1
Subtotal	**6**

Criterion 2: UniFi Floorplan Design And Logical Topology

Expected response	Marks
Imports or recreates the selected floorplan in UniFi Design Center and shows the property layout clearly.	1
Shows the internet/WAN entry point, modem/ONT, gateway/router and firewall function.	1
Includes a switch or PoE switch as the central wired LAN point for the star topology.	1
Places wireless access points in suitable locations.	1
Explains access point placement using floorplan, coverage, distance, wall or room-use reasons.	1
Labels wired ethernet, PoE/backbone links and wireless coverage/media where relevant.	1
Includes fixed high-demand or shared devices such as desktop, TV/media, NAS, printer, cameras, console or home office dock where suitable.	1
Shows or explains guest, IoT, home office, family or security camera network separation where suitable.	1
Provides UniFi Design Center coverage evidence such as	1

heatmap or coverage screenshots.	
Provides UniFi Design Center device placement, device list or export evidence.	1
Provides a readable logical topology using appropriate network diagram labels and conventions.	1
Keeps the final diagram/evidence readable, organised and suitable for client communication.	1
Subtotal	**12**

Criterion 3: Hardware, Network Type And Transmission-Media Decisions

Expected response	Marks
Explains the function of gateway/router, switch, firewall, modem/ONT, wireless access point and NIC; bridge or mesh is explained if used.	2
Recommends suitable high value domestic hardware, such as gateway/controller, PoE switch, ceiling or wall access points, outdoor access point, cameras, NAS or cellular backup where justified.	1
Justifies the selected hardware using the selected floorplan and client requirements.	1
Identifies and explains relevant network types, including LAN and WAN; PAN is identified only where it genuinely applies.	1
Explains why a star topology suits the domestic LAN design.	1
Recommends suitable transmission media such as twisted pair ethernet, fibre/ISP connection, wireless, cellular backup or satellite where justified.	1
Explains client-server or peer-to-peer technologies in relation to cloud services, NAS/media sharing, smart home control or home office use.	1
Subtotal	**8**

Criterion 4: Protocols, Security And Malware Response

Expected response	Marks
Explains SMTP as the protocol used to send outgoing email.	1
Explains IMAP and/or POP3 in relation to home office or cloud email use, with IMAP identified as suitable for multi-device mailbox access.	1
Recommends authentication controls for Wi-Fi, admin access, family users, guests or home office accounts.	1
Recommends encryption controls such as WPA2/WPA3, HTTPS, VPN or encrypted cloud services.	1
Recommends firewall controls or rules for traffic entering, leaving or moving between networks.	1
Recommends guest isolation, IoT isolation, VLANs or separate networks for privacy and security.	1
Identifies malware risks such as viruses, worms, trojans or spyware and gives relevant protection or response measures.	1
Links security decisions to personal privacy, home office data, cameras, smart home devices or household information.	1
Subtotal	**8**

Criterion 5: Justification, Communication And Submission Quality

Expected response	Marks
Justifies major design decisions using evidence from the selected floorplan and client requirements.	1
Connects the UniFi evidence, device choices and written explanation into a coherent final recommendation.	1
Uses accurate Computer Science terminology.	1
Organises evidence clearly so the source, UniFi design, topology and written justification align.	1
Submits the required files using the correct LMS process and file names.	1
Identifies limitations, testing evidence or future improvements such as heatmap uncertainty, extra cabling, wall assumptions or coverage checks.	1
Subtotal	**6**
Total	**40**

Moderation Notes

Do not award UniFi design marks for a floorplan that does not show network design evidence. Do not award topology marks for a floorplan alone. Do not award justification marks for generic claims that are not linked to the selected property, UniFi evidence or client requirements.